UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA

DONNA CURLING, ET AL.,

Plaintiffs,

v.

BRAD RAFFENSPERGER, ET AL.,

Defendants.

No. 1:17-CV-2989-AT

NOTICE

The undersigned counsel respectfully submit this notice on behalf of the United States Cybersecurity and Infrastructure Security Agency (CISA) in response to matters raised at the Court's February 2, 2022 hearing regarding CISA's Coordinated Vulnerability Disclosure (CVD) process. Specifically, CISA writes to provide additional information on the CVD process and its timeline, to reiterate its commitment to ensuring election security and completing the CVD process as quickly as feasible, and to notify the Court of CISA's view that premature disclosure of Dr. Halderman's report, even in redacted form, could, in the event any vulnerabilities ultimately are identified, assist malicious actors and thereby undermine election security. As explained herein, CISA thus respectfully submits that public disclosure, even in redacted form, should await completion of the normal CVD process and proposes that it notify the Court within 30 days of any status updates regarding the process and its anticipated timeline, as well as any updates regarding CISA's views as to scope and information to be included in a future public disclosure.

CISA understands that, during the February 2nd hearing, the Court authorized disclosure to CISA of an unredacted report prepared by Dr. Halderman for the purpose of CISA

undertaking its CVD process. CISA received an unredacted copy of the report from Dr. Halderman on February 2nd, and counsel for Plaintiffs shared the unredacted report with Dominion Voting Systems on February 4th. The report discusses potential vulnerabilities in Dominion ImageCast X ballot marking devices. *See generally* ECF 1177-1 ¶ 2.

Now that the report has been shared among Dr. Halderman, CISA, and Dominion, CISA has commenced its CVD process, which is described in detail in CISA's January 20, 2022 letter, *see* ECF No. 1269. CISA understands and shares the parties' urgency with completing this work, and will prioritize its completion as expeditiously as possible. As confirmed in CISA's letter, the CVD process requires the agency to coordinate between and work with the reporting source of the potential vulnerabilities (here, Dr. Halderman) and the vendor (here, Dominion), to analyze the potential vulnerabilities, including the risk they present; develop mitigation measures to mitigate the risk of the potential vulnerabilities, as needed; facilitate sufficient time for affected end users to obtain, test, and apply any recommended mitigation measures prior to full public disclosure of the potential vulnerability; and strive to ensure accurate and objective disclosures by the vendors. *See generally id.*[1] A range of factors—such as the potential impact on critical infrastructure (*e.g.*, election equipment), the availability of effective mitigations, the feasibility of developing an update or patch, the estimated time necessary for affected end users to obtain, test, and apply the patch, or other situations that require changes to established standards—may result

[1] CISA is also aware that, prior to and separate from the commencement of the CVD process, the Court imposed a protective order on dissemination of Dr. Halderman's report, as applied to parties in the litigation. As noted in CISA's letter, ECF No. 1269 at 2-4, the CVD process requires sharing and dissemination of vulnerability information. CISA understands the Court to have authorized disclosure of Dr. Halderman's report to CISA for the purpose of following its normal process, including, as appropriate, any information-sharing with Dr. Halderman, Dominion, affected end users, and, at the conclusion of the process, with the public. *See* Feb. 2, 2022 Hr'g Trans. at 5:12-20; 9:19-10:2.

in shifts to both the timeline and process. *See id.* Depending on what is discovered, CISA may need to coordinate with one or more affected end users, including states and municipalities using the same technology, early in the CVD process.

Both from the transcript of the February 2nd hearing and from a February 3rd conversation between undersigned counsel and the parties, CISA understands that the parties to this case requested a redacted version of Dr. Halderman's report to be released publicly as soon as possible. Specifically, the plaintiffs apparently request release of the redacted report within 30 days, while the State would prefer immediate (or as soon as practicable) release. CISA also understands that the Court would like to ascertain how quickly CISA can complete its process and whether CISA will be prepared to provide its views on what information may be released publicly without compromising security and what information should be withheld.

As to the timeline for the CVD process, CISA is not able to provide a definitive answer at this point. As with all of its CVD work, CISA's goal is to facilitate an assessment of the potential vulnerabilities in a coordinated way that minimizes risk. If warranted, CISA will coordinate with the vendor during development of any patches or other mitigation measures necessary to address any identified vulnerabilities. The rapidity with which that can be completed depends largely on the scope of any identified vulnerabilities, the actions and responses among participants in the process (*i.e.*, Dr. Halderman, Dominion, and states and municipalities using the same technology), the mitigation measures any identified vulnerabilities may warrant, and other factors, including the feasibility of, and timeline for, developing any needed update(s) or patch(es). Any mitigation measures also must be made available to affected end users—*i.e.*, both Georgia and other states/municipalities using the same technology—and must be obtained, applied, and tested by those stakeholders, as well as, in some cases, certified for use by those

stakeholders. Election security is a top priority; CISA is thus committed to taking these steps expeditiously and will seek to complete the process as promptly as possible. But the timeline also depends on the actions of a range of other actors outside CISA's control. A 30-day timeline may be impractical in this situation, despite best efforts and prioritization of this work.

CISA understands the urgency given the upcoming elections in which this voting equipment is presently planned to be used. Yet CISA can neither control how quickly any necessary mitigation measures are developed, made available, and implemented, nor at this time can CISA anticipate with any degree of reasonable certainty how long the process may take. This was communicated by undersigned counsel to counsel for the parties and counsel for Dominion during the February 3, 2022 conference call.

As to what can be released publicly, CISA supports public disclosure of any vulnerabilities and their associated mitigations, subsequent to any applicable mitigation measures being developed and applied, consistent with the CVD process. ECF No. 1269 at 3. As explained in CISA's January 20, 2022 letter, CISA carefully stewards sensitive data made available to the agency as part of the CVD process, maintaining confidentiality until disclosure to affected end users and the public at large is warranted. This enables key vulnerabilities to be addressed, while also preserving the confidentiality of sensitive proprietary information. Consistent with this approach, CISA typically would not release a report such as Dr. Halderman's at the conclusion of the CVD process; it would, however, disclose necessary information about any vulnerabilities and associated mitigations.

CISA is particularly concerned about dissemination of potential vulnerabilities—even in redacted form—before CISA and the vendor have been able to address them through appropriate mitigation action. Such premature disclosure increases the risk that malicious actors may be able

to exploit any vulnerabilities and threaten election security. CISA respectfully submits that, in order to best promote the security of the nation's critical infrastructure, any vulnerabilities should be disclosed—with the maximum appropriate transparency—in accordance with the CVD process. CISA's goal is to disclose any confirmed vulnerabilities and associated mitigations to the public in a coordinated way, so the entire cyber ecosystem can benefit while minimizing the risk of harm to election security.

For these reasons, CISA respectfully submits that public disclosure, even in redacted form, should await completion of the normal CVD process. CISA is committed to prioritizing this work and ensuring it is given the attention it deserves. CISA proposes that it notify the Court within 30 days of any status updates regarding the process or the anticipated timeline for completion, as well as any updates regarding CISA's views as to scope and information to be included in a future public disclosure.

Respectfully submitted,

BRIAN M. BOYNTON
Acting Assistant Attorney General

BRIGHAM J. BOWEN
Assistant Branch Director

/s/ Kate Talmor
KATE TALMOR
Trial Attorney
Civil Division
Federal Programs Branch
US Department of Justice
1100 L St., NW
Washington, DC 2005
202-305-5267
kate.talmor@usdoj.gov